Abstract of **CN1419363**

The present invention discloses a multicast control method based on 802.1X protocol. This method is to capture the message emitted by the authenticated user who wants to join the multi-broadcasting group. Then it obtains the port and the MAC address of the user from the captured message, searching the corresponding user's account number information from the authenticated data by means of the portand the MAC address. After passing the authentication of the account number and the IP address, the user can be added to the multicast. The method can realize the controlled multicast, the validity authentication and the charge calculation on the user's joining to the multicast, and in favor of protecting the compatibility of the user's current investment and the existing software.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 29/06
H04L 12/18

[12] 发明专利申请公开说明书

[21] 申请号 02154612.6

[43] 公开日 2003 年 5 月 21 日

[11] 公开号 CN 1419363A

[22] 申请日 2002.11.26 [21] 申请号 02154612.6

[71] 申请人 华为技术有限公司

地址 518057 广东省深圳市南山区科技园科发路 1 号

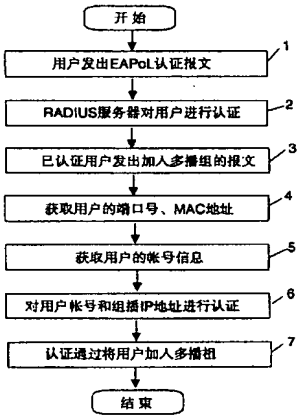
[72] 发明人 罗汉军 卢瑞昕

权利要求书 1 页 说明书 7 页 附图 2 页

[54] 发明名称 基于 802.1X 协议的组播控制方法

[57] 摘要

本发明公开了一种基于 802.1X 协议的组播控制方法，该方法在通过认证的用户发出加入多播组的报文时，截获该报文，然后从截获的报文中获取用户的端口和 MAC 地址，利用上述端口和 MAC 地址从已认证的数据中查找对应的用户账号信息，再对用户的账号和组播 IP 地址进行认证，认证通过后将该用户添加到多播组；上述方案能实现受控组播，对用户组播加入进行合法性认证和计费，并且有利于保护用户已有投资和现有软件的兼容。



ISSN1008-4274

1、一种基于802.1X协议的组播控制方法，包括：

步骤1：当通过认证的用户发出加入多播组的报文时，截获该报文；

步骤2：从截获的报文中获取用户的端口和MAC地址；

步骤3：利用上述端口和MAC地址从已认证的数据中查找对应的用户账号信息；

步骤4：对用户的账号和组播IP地址进行认证，认证通过后将该用户添加到多播组，否则拒绝。

2、根据权利要求1所述的基于802.1X协议的组播控制方法，其特征在于，所述方法还包括：采用802.1X认证端的认证服务器对用户的账号和组播IP地址进行认证。

3、根据权利要求2所述的基于802.1X协议的组播控制方法，其特征在于，在对用户的账号和组播IP地址进行认证时，通过检查组播IP地址是否被授权接收该帐号用户完成认证。

4、根据权利要求1所述的基于802.1X协议的组播控制方法，其特征在于，如果802.1X协议基于端口认证，挂接在该端口下的用户申请加入多播组时，首先查询该用户的MAC地址是否存在，如果存在，则根据找到的该用户的MAC地址和端口号查找用户账号。

如果802.1X协议基于MAC认证，挂接在该端口下的用户申请加入多播组时，直接根据用户的MAC地址和端口号查找用户账号。

5、根据权利要求1、2、3或4所述的基于802.1X协议的组播控制方法，其特征在于，用户使用IGMP协议进行多播组的加入。

基于802.1X协议的组播控制方法

技术领域

本发明涉及通信网络的组播控制方法，尤其是涉及基于802.1X协议的组播控制方法。

背景技术

在通信网络中，对于交换机或路由器等数据转发设备来说，对转发的网络数据采用对应用户分组的方式进行转发，有利于数据安全和网络资源的利用。例如，假设网络中有一多播组G，在路由器转发多播组G的数据一段时间后，会发出一个查询消息，看网络上是否还存在多播组G的成员，已经加入多播组G的成员要重新发布IGMP（因特网组管理协议）加入消息来作为成员查询消息的响应，当网络中没有多播组的成员时，路由器将收不到响应，此时路由器将再次进行查询尝试，如果还没有得到应答，就认为网络上已经没有多播组G的成员，于是停止转发多播组G的数据。由于采用上述多播组的管理方式，数据的转发相对于广播方式来说更有针对性，因此数据的安全和转发效率也更高。

但是在目前广泛使用IEEE 802.1X协议的局域网中，对于组播的控制只能基于端口完成，即通过将端口加入多播组的方式实现用户加入多播组。当用户主机发起加入多播组的请求时，网络交换设备根据情况将相应用户主机的MAC地址加入多播组，从而完成用户多播组的加入。由于这种方法只能提供端口号和用户主机的MAC地址，根本无法提供用户信息，而没有用户信息导致无法进行与用户有关的控制 。尽管IEEE 802.1X协议是一种基于端口的网络访问控制协议，可以针对用户进行管理，一个端口可以容纳多个用户认证，但是目前还无法利用上述特点控制

用户的组播加入，即控制用户加入多播组，从而导致用户组播加入的不可控性。

发明内容

本发明的目的在于提供一种基于802.1X协议的组播控制方法，使用该方法能够实现用户组播加入的可控性。

为达到上述目的，本发明提供的基于802.1X协议的组播控制方法，包括：

步骤1：当通过认证的用户发出加入多播组的报文时，截获该报文；

步骤2：从截获的报文中获取用户的端口和MAC地址；

步骤3：利用上述端口和MAC地址从已认证的数据中查找对应的用户账号信息；

步骤4：对用户的账号和组播IP地址进行认证，认证通过后将该用户添加到多播组，否则拒绝。

所述方法还包括：采用802.1X认证端的认证服务器对用户的账号和组播IP地址进行认证。

在对用户的账号和组播IP地址进行认证时，通过检查组播IP地址是否被授权接收该帐号用户完成认证。

如果802.1X协议基于端口认证，挂接在该端口下的用户申请加入多播组时，首先查询该用户的MAC地址是否存在，如果存在，则根据找到的该用户的MAC地址和端口号查找用户账号。

如果802.1X协议基于MAC认证，挂接在该端口下的用户申请加入多播组时，直接根据用户的MAC地址和端口号查找用户账号。

在上述方案中，用户使用IGMP协议进行多播组的加入。

由于本发明在通过802.1X协议认证的用户要求加入多播组时，首先拦截该加入多播组的报文，此时，并不直接将该用户增加到多播组，而是将

从截获的报文中获取该用户的端口和MAC地址，再利用上述端口和MAC地址从已认证的数据中查找对应的用户账号信息，然后将该用户的账号和组播IP地址再次进行认证，认证通过后才将该用户添加到多播组，否则拒绝；这种方案能实现受控组播，对用户组播加入进行合法性认证和计费；另外，这种方法不需要修改组播客户端软件和服务器软件，只需在802.1X设备端和认证端的认证服务器上进行简单的设置即可实现，有利于保护用户已有投资和现有软件的兼容。

附图说明

图1是802.1X协议的体系结构图；

图2是基于802.1X认证的受控组播体系图；

图3是基于802.1X认证的受控组播认证过程图；

图4是本发明所述方法的实施例流程图。

具体实施方式

下面结合附图对本发明作进一步详细的描述。

首先参考图1。图1所采用的IEEE 802.1X协议是一种基于端口的网络访问控制协议，用于在网络设备的物理接入级对接入客户端进行认证和控制。图1中共有三个实体：802.1X客户端、802.1X设备端、认证端。在802.1X设备端和认证端的认证服务器之间采用可扩展的认证协议（EAP）交换认证信息。EAPoL是802.1X客户端和802.1X设备端间的认证协议。通常，在网络的接入层设备需要实现802.1X的设备端部分；802.1X的客户端安装在用户PC中；802.1X的认证服务器系统一般驻留在运营商的AAA(计费、认证和授权）中心。在802.1X设备端内部有受控端口（Controlled Port）和非受控端口（Uncontrolled Port）。非受控端口始终

处于双向连通状态，主要用来传递 EAPoL协议帧，可保证随时接收和发送EAPoL 协议帧。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。受控端口可配置为双向受控、单向受控两种方式，以适应不同的应用环境。在上述体系结构下，如果采用以太网交换机或宽带接入设备实现802.1X设备端，则连接在以太网交换机或宽带接入设备端口上客户端的用户设备如果能通过认证，就可以访问网络内的资源；如果不能通过认证，则无法访问网络内的资源。上述端口可以是物理端口，也可以是逻辑端口，例如，在以太网交换机的一个物理端口连接一台客户端计算机就是一种典型的应用方式。

在图1所示的体系中，目前在802.1X设备端和认证服务器之间也可以运行的Radius（远程用户拨号认证）协议，因此，认证服务器为Radius服务器(Radius Server)，802.1X设备端可以看作Radius服务器的客户端。

由上述可知，在图1所示的体系中，如果以太网交换机将用户通过802.1X客户端发出的EAPoL-Start报文透传到802.1X设备端后，会触发802.1X协议对用户的认证。当认证端的认证服务器对用户的认证通过后，802.1X设备端的受控端口即可打开，用于为用户传递网络资源和服务，从而使用户处于网络在线阶段。假设一在线用户的主机想加入一个多播组，于是该用户主机通过组播客户端软件发出一个IGMP（假设采用该协议，但实际中用户加入多播组并局限于仅使用该协议）的加入消息给作为设备端的以太网交换机，告诉以太网交换机自己想加入该多播组，进而使以太网交换机开始转发该多播组的数据给发出消息的用户主机。

因此，只要当用户通过基于802.1X协议的认证，即可完成802.1X协议对该用户的网络连接，在此基础上，如果用户要加入多播组，就可以从用户基于上述连接的加入多播组的消息或报文中获取用户主机的MAC地址

和端口号，这样就可以利用所述MAC地址和端口号从用户的认证数据中获取用户的详细信息，实现组播加入的控制，从而解决现有方法的组播加入的不可控问题。

本发明的原理参考图2。图2所示的以太网交换机用于连接图1所示的客户端，并且用于实现图1所示的设备端，因此该以太网交换机将用于客户端网络连接通道的开关控制。由于连接在以太网交换机端口上的用户未通过认证时该端口不能使用，而通过认证用户认证的端口可以自动动态配置并访问网络资源，这就给图2所示的基于802.1X协议的以太网交换机为运营商带来了可运营特征。图2中，作为802.1X的设备端的以太网交换机采用Radius协议模块与认证端的Radius服务器传递认证信息。802.1X认证模块用于从交换机的相应端口接收用户发出的基于802.1X的认证信息，并将所述认证信息通过Radius认证模块传递到认证端的认证服务器进行认证，该认证信息中包括用户的详细信息，如用户名、密码等。如果认证通过，则不但在已认证的信息中包括该用户的详细信息，而且也会使802.1X认证模块开通连接该用户的端口业务通道（相当于接通图2中的开关K1），这样用户就可以通过该端口业务通道访问网络资源，即该用户已经完成了基于802.1X的网络连接。在上述802.1X连接的基础上，如果用户通过端口业务通道发出加入多播组的报文或消息，假设为基于IGMP协议的报文，则可以通过设置使以太网交换机中的组播控制模块拦截该IGMP报文，获取其中用户的MAC地址和端口号，然后利用上述MAC地址和端口号从该用户的802.1X连接中获取用户账号信息（用户名、密码等），然后根据用户信息和组播IP地址建立受控组播连接，即，使组播控制模块根据控制的需要控制组播开关K2的打开或闭合。可见，通过将组播与802.1X认证通过的端口和用户MAC地址结合起来，就可以实现用户组

播加入的可控性。具体到图2，802.1X认证模块负责端口业务通道开关K1的控制，组播控制模块负责端口业务通道的组播开关K2的控制。

图4是本发明所述方法的实施例流程图。图4描述的基于802.1X认证的受控组播认证过程参考图3，图4所述的实施例假设用户采用IGMP报文加入多播组，并且预先已设置好交换机中的组播控制模块在用户发出IGMP报文后首先获取该报文。按照图4，首先用户在步骤1上网初始时通过EAPoL报文触发802.1X设备端的802.1X协议认证，即，EAPoL报文被透传到作为802.1X设备端的以太网交换机的802.1X认证模块，然后802.1X认证模块在步骤2将用户的认证信息通过Radius模块与认证端的Radius服务器进行认证。认证通过后，将认证通过的用户信息保存到以太网交换机中，如保存到802.1X认证模块中。上述两个步骤主要用于完成用户的认证过程，使用户处于网络在线状态。如果通过认证的用户在步骤3发出IGMP报文要求加入一多播组，则组播控制模块在步骤4拦截用户发出的加入多播组的IGMP报文，此时，组播控制模块并不直接将该用户增加到多播组，而是将从IGMP报文中截获的该用户的端口号、MAC地址发送给802.1X认证模块，802.1X认证模块利用上述端口和MAC地址在步骤5从已认证的数据中查找对应的用户账号信息，找到后将该用户账号信息反馈给组播控制模块，然后组播控制模块将该用户的账号和组播IP地址在步骤6再次通过Radius模块送到认证端的Radius服务器进行认证，也就是利用用户的账号和组播IP地址进行认证，通过检查组播IP地址是否被授权接收该帐号用户完成认证，认证通过后才在步骤7将该用户添加到多播组，否则拒绝。在用户加入多播组后，组播控制模块维持该组播连接，直到用户请求退出。

需要说明，由于目前的以太网交换机基于802.1X协议的认证方式有基于端口和基于MAC地址两种方式，因此要对这两种方式区别对待。对于基于端口的认证方式，在该认证模式下，每个端口802.1X模块只控制一

个认证用户，所以只维持一个802.1X连接，但通过802.1X认证后，该端口可以下挂多台用户的PC，因此挂接在端口下的用户PC申请加入多播组时，采用替换MAC方式，即首先向802.1X模块查询该用户的MAC地址是否存在，如果存在说明该用户已通过认证，则802.1X返回认证用户的MAC地址，组播控制模块根据返回的MAC地址和端口号查找用户账号。

对于基于MAC地址的认证方式，802.1X模块对端口下挂的每台PC都已认证通过，且都有连接对应，因此挂接在该端口下的用户申请加入多播组时，直接向802.1X模块查询该MAC地址，802.1X模块返回该MAC地址后，再根据该MAC地址和端口号查找用户账号，所以每个用户都能通过各自的MAC地址和端口号找到相应的802.1X连接，即都可以获取用户账号信息。

图4所述的实施例采用Radius服务器管理用户的信息，因此本实施例也采用Radius服务器对用户的组播加入进行控制，具体通过在Radius服务器中增加受控组播属性项实现，即在Radius服务器上配置用户账号，然后给该账号增加增值组播服务项目。利用该属性项可以为用户增加一个或多个组播地址，当Radius服务器接收到包括用户帐号和组播IP地址的认证请求时，若有受控组播属性项目，则检查组播IP地址是否被授权，若已授权则返回成功，否则反馈认证失败。

因此可以通过将组播业务属性项作为用户的增值业务属性，附属在用户帐户上，首先增加用户，然后再给该用户开通组播频道。这样，通过本发明就可以为运营商提供组播增值服务，将基本的802.1X上网认证连接计费和增值的组播服务计费分开，便于不同服务提供商间的结算。

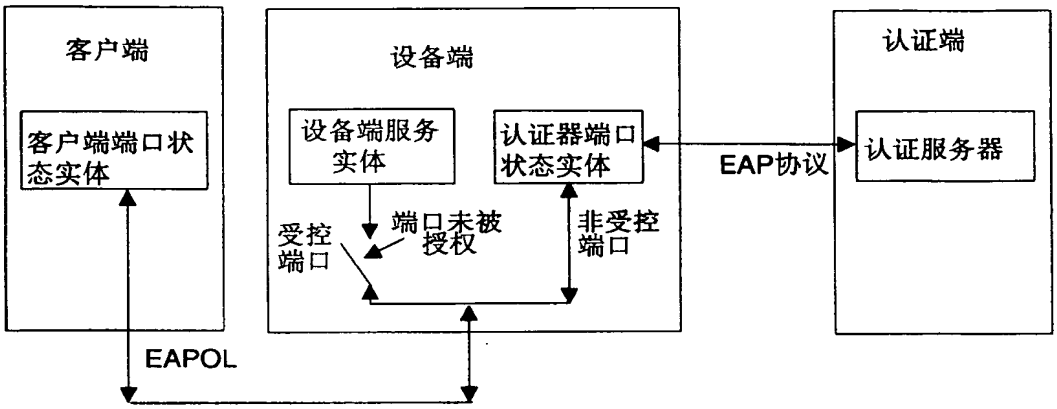

客户端
客户端端口状态实体
设备端
设备端服务实体
认证器端口状态实体
受控端口
端口未被授权
非受控端口
EAP协议
认证端
认证服务器
EAPOL

图1

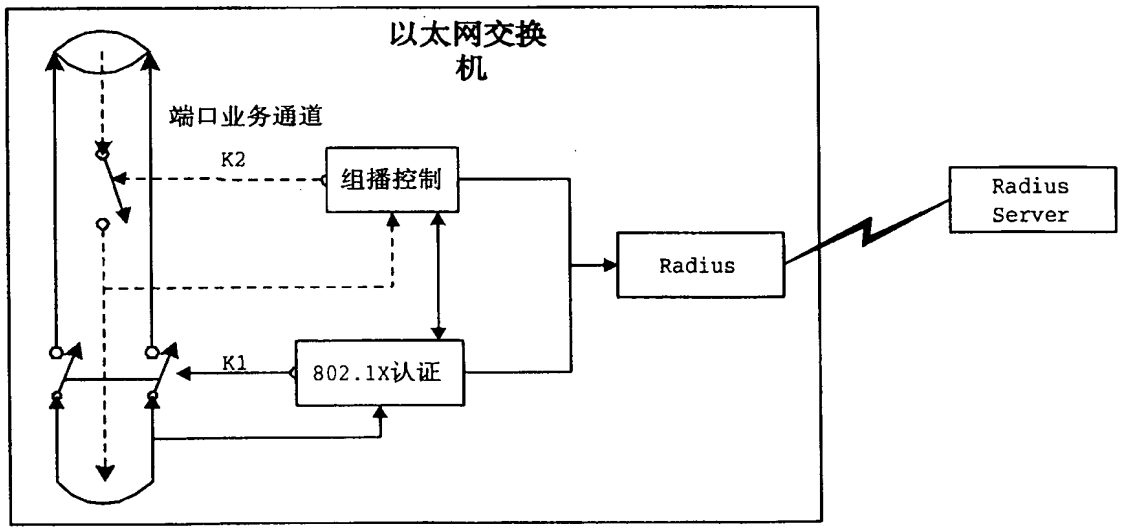

以太网交换机
端口业务通道
K2
组播控制
Radius
Radius Server
K1
802.1X认证

图2

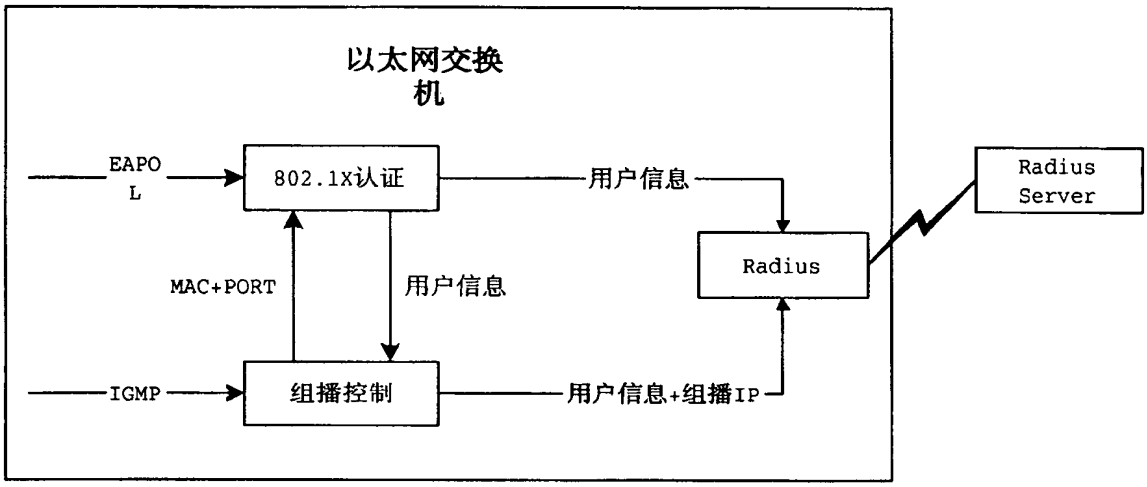

以太网交换机
EAPOL
802.1X认证
用户信息
Radius Server
Radius
MAC+PORT
用户信息
IGMP
组播控制
用户信息+组播IP

图3

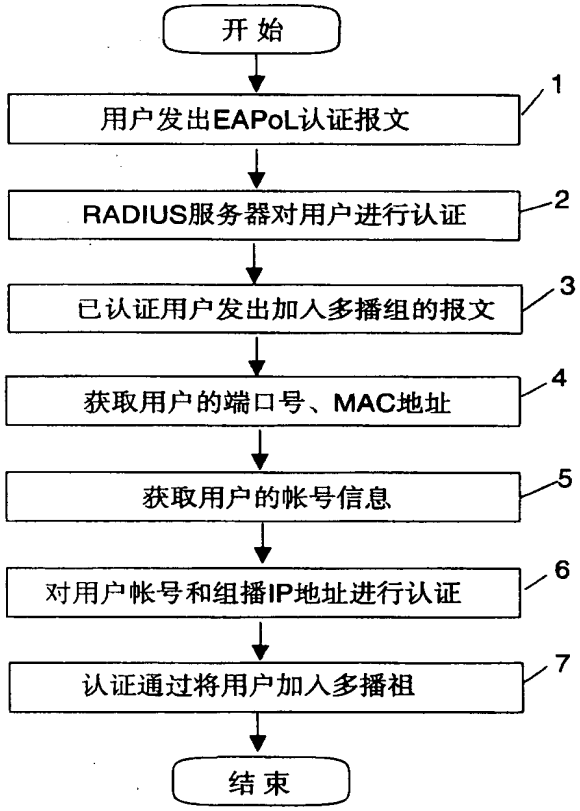

开始
用户发出EAPoL认证报文
1
RADIUS服务器对用户进行认证
2
已认证用户发出加入多播组的报文
3
获取用户的端口号、MAC地址
4
获取用户的帐号信息
5
对用户帐号和组播IP地址进行认证
6
认证通过将用户加入多播祖
7
结束

图4